Department of Homeland Security Daily Open Source Infrastructure Report for 19 October 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Honolulu Advertiser reports the recent Oahu−wide blackout was caused when Hawaiian Electric Co. was unable to adjust to the unexpected shutdown of two power generators that represented just 12 percent of generating capacity; the utility malfunctioned and shutoff power to the entire island. (See item 4)
- A RAND Corporation study warns the maritime terrorism risk extends beyond dangers posed to container shipping, and cruise ships and ferry boats need more protection against terrorist attacks that could kill and injure many passengers and cause serious financial losses. (See item 16)
- US−CERT has released Technical Cyber Security Alert TA06−291A: Oracle updates for multiple vulnerabilities (See item 36)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *October 18, Knoxville News Sentinel (TN)* — **Crackdown on nuke workers.** Several nuclear workers were found sleeping, playing cards, and watching TV last week at the Molten Salt Reactor, an old experimental reactor at Oak Ridge National Laboratory. The men were

subcontractors of the Department of Energy (DOE) who were preparing to remove tons of highly radioactive fuel salts stored there since the reactor was shut down in 1969. According to Dennis Hill, a spokesperson for Bechtel Jacobs, DOE's cleanup manager, a visit to a break trailer outside the reactor confirmed that there were also indications that marijuana had been smoked in the trailer. During a tour of the parking lot, drug dogs "hit" on four different vehicles, one of which contained an unspecified amount of marijuana, Hill said. More than 50 people working on the Molten Salt Reactor project were required immediately to take drug tests. Most nuclear work at the Molten Salt Reactor has been suspended for several months because of a fluorine leak earlier this year. The cleanup plan called for additional training this fall and restart of fuel−removal tasks in November. It was not immediately clear if the latest incident would alter that schedule.
Source: http://www.knoxnews.com/kns/local_news/article/0,1406,KNS_34 7_5073819,00.html

2. *October 17, WABC−TV 7 (NY)* — **LIPA to spend $500 million to upgrade system.** The Long Island Power Authority (LIPA) says it will spend $500 million dollars to reduce damage from severe storms. If it works, it's great news for anyone who uses electricity. When Ernesto's remnants came knocking in September, it toppled trees and power lines leaving tens of thousands in the New York area without power. Thankfully, LIPA preplanned. "We did do well this summer because we have invested heavily into the infrastructure," a LIPA official said. LIPA says every tree on Long Island interfering with a power line will get a trim and some substations will be raised to protect against flooding.
Source: http://abclocal.go.com/wabc/story?section=local&id=4670694

3. *October 17, KRQE News 13 (NM)* — **Tower collapse kills worker.** One power−line worker died and another was critically injured Tuesday, October 17, when they fell at least 50 feet with a collapsing transmission tower. The men were setting up an emergency tower as part of a demonstration for an international power industry conference hosted by PNM in Albuquerque. Two men were demonstrating how to construct a temporary transmission tower used to quickly restore power in an emergency. “It was a tower that’s utilized in emergency restorations of a transmission tower,” Eddie Padilla of PNM said. “They were demonstrating how to erect this tow[er] for emergency situations.”
Source: http://www.krqe.com/expandedb.asp?RECORD_KEY%5Bnewsb%5D=ID&ID%5Bnewsb%5D=17709

4. *October 16, Honolulu Advertiser* — **Oahu blackout similar to major Mainland interruptions.** The Sunday, October 15, power outage on the Hawaiian Island of Oahu resembled large Mainland blackouts in which a minor problem multiplies into a major power problem. Cascading blackouts can be triggered, as in the case of Sunday's outage, by an earthquake−induced shutdown of just two of 13 power generators. While rare, such systemwide electricity shutdowns can happen. Just why the earthquake, which did not cause any significant structural damage, caused such a major blackout is still unclear. However, the blackouts likely were exacerbated by the state's geographically isolated power grid and tremors. On the Mainland, a similar systemwide shutdown may not have had as significant an impact because electricity can be brought in from other states, said Dennis Murphy of GE Energy. That's not an option in Hawaii. Sunday's Oahu−wide blackout was caused when Hawaiian Electric Co. was unable to adjust to the unexpected shutdown of two power generators that represented just 12 percent of generating capacity. Rather than cut power to 12 percent of customers, the utility

shutoff power to the whole island. Utility grids are designed with automated systems capable of adjusting to withstand such incidents, but as Sunday's blackout illustrates, these systems don't always work as planned.
Source: http://the.honoluluadvertiser.com/article/2006/Oct/16/br/br8 341057269.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *October 18, Telegraph (GA)* — **Truck with lighters wrecks, catches on fire.** A tractor−trailer carrying butane lighters overturned Wednesday morning, October 18, in Macon−Bibb County, GA, causing a fire and blocking off Interstate 75 north at the Interstate 16 east interchange for several hours as emergency response crews worked to clear the scene. The driver of the truck apparently swerved and lost control of the vehicle, causing it to overturn. Inside the truck, the lighters caught on fire. The driver of the truck was not injured, and no other cars traveling at the same time were involved with the wreck.
Source: http://www.macon.com/mld/macon/news/breaking_news/15788577.h tm

6. *October 18, Associated Press* — **Emergency crews return to North Carolina chemical plant to combat small fire.** Emergency crews in Apex, NC, evacuated several businesses while they fought a small fire Wednesday, October 18, at a chemical plant where a raging inferno forced thousands from their homes two weeks ago. The blaze was contained to a 55−gallon barrel on the property, but it was smoky and the fumes were irritating, said Mayor Keith Weatherly. The chemical drum contained a sodium metal solution that can ignite when exposed to water or air. The area had been drenched by rain on Tuesday. The chemical plant belonging to EQ Industrial Services Co. previously caught fire October 5, lighting up the sky with explosions and blanketing parts of the town in a yellow−green haze. Town officials had urged as many as 17,000 people to evacuate, citing potentially toxic fumes that had made a few dozen people seek medical attention.
Source: http://www.kcbs.com/topic/ap_news.php?story=AP/APTV/National /a/a/PlantFire−Evacuation_a_a_−−−−−

7. *October 18, Associated Press* — **Three hurt in explosion at tanker−trailer business in Texas.** An explosion tore through a business where tanker−trailers are made Wednesday, October 18, seriously injuring two men, damaging three nearby buildings and blowing out windows throughout an industrial area of the Lubbock, TX. Officials at University Medical Center said a 57−year−old man suffered multiple lacerations and a 64−year−old man suffered chemical burns. Police Lt. Scott Hudgens said a third man suffered minor injuries when a light fixture fell on him at a nearby funeral home. The cause of the midmorning blast inside the Harmon Tank Company is being investigated.
Source: http://www.dfw.com/mld/dfw/news/state/15789534.htm

[Return to top]

Defense Industrial Base Sector

8. *October 18, U.S. Air Force* — **President signs 2007 Defense Authorization Act.** The fiscal 2007 National Defense Authorization Act provides more than $530 billion to maintain the military in the shape it must be to win the war on terrorism. President Bush signed the bill, officially called the John Warner National Defense Authorization Act for Fiscal Year 2007, during a small ceremony in the Oval Office Tuesday, October 17. The act provides $462.8 billion in budget authority for the Department of Defense. Senate and House conferees added the $70 billion defense supplemental budget request to the act, so overall, the act authorizes $532.8 billion for fiscal 2007.
Source: http://www.af.mil/news/story.asp?id=123029372

[Return to top]

Banking and Finance Sector

9. *October 18, Stars and Stripes* — **Military credit unions warn of phishing scams in e−mails.** Military credit unions are again warning members not to fall victim to e−mail scams asking for customers' financial and personal information. In the last week, both the Navy Federal Credit Union and the Marine Federal Credit Union have posted warnings about e−mail phishing scams where unknown opportunists are posing as employees asking for credit card numbers, financial information, and passwords for alleged account verification. In the latest scam, an e−mail informs Marine credit union customers that their accounts have been locked because "it may have been compromised by outside parties" and links to an unsecured Website which includes a copy of the credit union's logo.
Source: http://www.estripes.com/article.asp?section=104&article=4082 2

10. *October 18, VNUNet* — **Haxdoor mutates to steal confidential info.** New variants of the Haxdoor Trojan have been discovered in the wild, security firm Panda Software has reported. The mutants are particularly dangerous because they use a rootkit to hide their actions and avoid detection. Several new versions of the Haxdoor family of Trojans have emerged over the past few days. The malware tries to steal confidential user details in order to commit online fraud and identity theft. The latest strains have several common characteristics, including a capacity to install a rookit designed to hide objects, such as processes, files or entries. Haxdoor uses this rootkit to hide itself on the computer from the user and the majority of traditional security systems. All the new variants are designed to steal passwords for popular Internet services, such as eBay, ICQ, PayPal and WebMoney, and for many email clients, including Outlook Express and The Bat. "It seems that the authors of these malicious codes are mass−mailing these Trojans as attachments to spam messages," said Luis Corrons, director of PandaLabs.
Source: http://www.vnunet.com/vnunet/news/2166702/trojan−variants−hu nt

11. *October 17, Tribune (CO)* — **Colorado funds ID theft task force.** Colorado has passed legislation (House Bill 1347) instituting a state−funded, statewide, interagency, law enforcement task force protecting people from identity theft. The newly−created Colorado Identify Theft Unit helps people avoid identity theft and assists law enforcement agencies in tracking down, arresting and convicting identity thieves.
Source: http://www.greeleytrib.com/article/20061017/NEWS/61017004

12. *October 16, Websense Security Labs* — **Multiple Phishing Alert: Lorain National Bank, Bank of the Cascades, Great Western Bank.** Websense Security Labs has received several reports of phishing attacks that target banking customers. All phishing e−mails below provide a link to a phishing site that attempts to collect user account information.
Lorain National Bank: Users receive a spoofed e−mail message, which claims that the services listed on the e−mail will be deactivated if not renewed immediately. Users are asked to log on to prevent their services from being suspended.
Bank of the Cascades: Users receive a spoofed e−mail message which claims that, due to an irregularity in the way a credit card has been used on their account, some limitations have been applied. In order to remove the limitations, users are asked to verify and confirm their details.
Great Western Bank: Users receive a spoofed e−mail message which claims that if they take part in a survey, $100 will be credited to their account.
Screenshots:
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=666
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=665
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=664
Source: http://www.websense.com

[Return to top]

Transportation and Border Security Sector

13. *October 18, USA TODAY* — **TSA plan: X−ray for liquid bombs.** The Transportation Security Administration (TSA), in a potential strategy shift, may screen carry−on bags with new three−dimensional X−ray machines that are better at spotting liquid explosives, guns and other weapons. The 3−D machines have "an extraordinary ability to find" liquids, TSA chief Kip Hawley told USA TODAY. "They're a step beyond where we are today." The TSA has limited the volume of liquids passengers can carry on planes since authorities foiled a plot in London in August to bomb U.S.−bound planes with liquid explosives. Installing new X−ray machines would improve security and could ease the liquid restrictions, aviation consultant Richard Roth said. The question for the TSA is whether to buy upgraded X−ray machines for $75,000 to $200,000 each or to wait possibly two years for better machines costing about $400,000. The TSA had planned to wait for the more expensive machines, which have the highest level of explosives detection. The TSA will evaluate the machines in coming months. They provide more detailed images than the X−rays airports have used for 30 years. Those X−rays have been criticized by the Department of Homeland Security's inspector general for inadequately spotting explosives, guns and knives.
Source: http://www.usatoday.com/travel/news/2006−10−17−tsa−xray_x.ht m

14. *October 17, Gannett News Service* — **Border 'passport cards' could cost $20.** People who frequently go back and forth between the U.S. and Mexico or Canada would pay $20 for a new credit card−sized travel document they could use instead of a passport under a new government proposal. By June 2009, all U.S. citizens will need a passport or the new card to enter the country from Mexico or Canada. Mexican and Canadian citizens will need similar documents their countries will produce. The State Department proposed the card and its fee schedule Tuesday, October 17, and officials will take comments from the public for two months before moving ahead with production. The cards would use radio technology that would allow

Customs and Border Protection officers to read them from about 20 feet away. Passengers in a car driving across the border, for example, could have their information scanned without getting out. Border community residents had feared the passport requirement would prove to be an expensive and logistically taxing burden, but the State Department proposal eased some worries. The government will now have some extra time to process what could be millions of applications for the cards.
Source: http://www.usatoday.com/travel/news/2006−10−17−passport−card_x.htm

15. *October 17, Department of Homeland Security* — **DHS to expand use of vicinity RFID in Western Hemisphere Travel Initiative.** The Department of Homeland Security (DHS), in conjunction with the Department of State's proposed rulemaking on the new PASSport card, announced today that it proposes to expand the use of vicinity radio frequency identification (RFID) technology at U.S. ports of entry. The vicinity RFID technology, to be compatible with the PASSport card, would allow a travel document to be read from several feet as a vehicle approaches inspection. The PASSport card, part of the People Access Security Service (PASS) System, is designed to meet the specific requirements of the Western Hemisphere Travel Initiative (WHTI) for U.S. citizens crossing U.S. borders by land or sea. To protect the privacy of Americans who opt to use the PASSport card, no personal information will be stored or transmitted on the RFID chip on the card. The technology will transmit only a number between the card and the reader which will be matched against a DHS database. Vicinity RFID, which is also used successfully in highway toll systems across the United States, demands little of the traveler and can read multiple cards simultaneously inside a vehicle. The vicinity RFID technology will increase the security of the border while facilitating commerce at the port of entry.
Factsheet: http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm
Source: http://www.dhs.gov/xnews/releases/pr_1161114866740.shtm

16. *October 16, RAND Corporation* — **RAND study warns maritime terrorism risk extends beyond dangers posed to container shipping.** Cruise ships and ferry boats need more protection against terrorist attacks that could kill and injure many passengers and cause serious financial losses, according to a new RAND Corporation report entitled, Maritime and Terrorism: Risk and Liability. "Attacks on cruise ships and ferry boats would meet the interrelated requirements of visibility, destruction and disruption that drive transnational terrorism in the contemporary era," said Peter Chalk, one of the report's co−authors. "Recognizing this is essential to any comprehensive regime of maritime security." The report concludes it is not adequate to base maritime counterterrorism efforts only on increasing port security and the security of cargo container ships, rail cars and trucks that transport goods into and out of United States ports. The study by RAND, a nonprofit research organization, also says a maritime terrorist attack is likely to create complicated liability issues that will slow efforts to compensate victims of an attack. The report argues that attacks on passenger ferries or cruise ships would be more probable than a nuclear device smuggled inside a shipping container. These attacks might involve on−board bombs or biological contaminants inserted into the food supply, according to researchers.
Report: http://www.rand.org/pubs/monographs/MG520/
Source: http://www.rand.org/news/press.06/10.16.html

[Return to top]

Postal and Shipping Sector

17. *October 18, New England News* — **Mail carrier's death leads to discovery of undelivered mail.** When Alan J. Gagne, 20−year−veteran of the U.S. Postal service didn't return from deliveries in Brookline, MA, on Friday, October 13, his boss found he may not have been as dedicated to the route as they had thought. In his apartment, his boss found Gagne dead from an apparent heart attack. The supervisor also found stacks of undelivered mail stuffed in closets and cabinets. The oldest article so far was dated in the 1990s, according to Post Office officials. But as of Monday they had not finished cataloging the four or five truckloads of undelivered mail. "It's a mystery," Postal Service spokesperson Robert Cannon told The Boston Globe. "Why would he have all that? We don't know ... There are a lot of answers we don't have right now." The Postal Service's Office of Inspector General has deployed agents to sort and deliver the first class mail. Most of the mail was circulars and advertising, Cannon said, addressed to residents who had moved.
    Source: http://www1.whdh.com/news/articles/local/BO31344/

18. *October 18, WIFR (IL)* — **Emergency drill at post office.** A major bio−hazard training drill recently went well at the main Rockford, IL, post office. Post office administrators said they want employees to be as prepared for a bio−hazard emergency as they would be for a fire. In an actual emergency an alarm would signal a bio−hazard agent like Anthrax had been detected. The equipment constantly scans the air for bio hazards as new mail comes in to be postmarked. In this drill, members of the U.S. Post Inspections Service, Rockford Police and Fire Department, and the Winnebago County Department of Health came out to practice evacuating and securing the building.
    Source: http://www.wifr.com/home/headlines/4422606.html

19. *October 17, Memphis Business Journal* — **FedEx pilots ratify contract.** FedEx Express and the Air Line Pilots Association (ALPA) jointly announced Tuesday, October 17, that the pilots have voted to ratify the four−year contract FedEx proposed in September. FedEx Express is the global air carrier unit of Memphis−based FedEx Corp. ALPA represents FedEx Express pilots. The contract, which will take effect October 30, is the culmination of a negotiation process that began in 2004.
    Source: http://biz.yahoo.com/bizj/061017/1361738.html?.v=1

20. *October 16, Des Moines Register (IA)* — **West Des Moines, Iowa, police investigate suspicious pipe.** The West Des Moines Police Department and Bomb Squad are continuing to investigate the contents of a pipe found Monday afternoon, October 15, in a mailbox. Police were called to the 700 block of 42nd St. in West Des Moines when a mail carrier found a PVC pipe in the mailbox. Sgt. Russ Schafnitz from the Des Moines Police Bomb Squad said, “We knocked the end cap off of it,” Schafnitz said. “All I can say is that the device is suspicious and homemade,” Lt. Jeff Miller of the West Des Moines Police said. “Normally, we find a black powder or flash powder in these things,” Schafnitz said. “In this case, there was a gel inside the tube.”
    Source: http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20061016/NEWS/61016056/1001

[Return to top]

Agriculture Sector

21. *October 18, USAgNet* — **Six Illinois counties now have rust.** Illinois now has six counties with confirmed soybean rust outbreaks. The latest to be included are Johnson, Pulaski and Alexander counties in deep southern Illinois. The other counties with earlier finds are White, Massac and Pope.
Source: http://www.usagnet.com/story−national.php?Id=2162&yr=2006

22. *October 17, Agence France−Presse* — **Mad cow disease found in Russia.** A case of bovine spongiform encephalopathy or mad cow disease has been discovered in the Russian enclave of Kaliningrad between Poland and Lithuania, the Federal Control Service for Consumer Rights said. "A case of mad cow disease was detected in the town of Razdolnoye in the Nesterovski region," near the Lithuanian border, it said in a press release. In July 2005, Moscow announced it had found around 10 cases of mad cow disease in four farms in Mordovia, in the eastern European area of Russia.
Source: http://news.yahoo.com/s/afp/20061017/hl_afp/russiahealthmadcow_061017180030;_ylt=Ar.uY9Sw6nWDP95_kA20pDmJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

23. *October 17, U.S. Department of Agriculture* — **Avian influenza tests complete on green−winged teals in Illinois.** The U.S. Departments of Agriculture and Interior Tuesday, October 17, announced final test results, which confirm that a low pathogenic avian influenza (LPAI) virus was found in samples collected last month from wild green−winged teals in Illinois. LPAI has been detected several times in wild birds in North America and poses no risk to human health. The USDA National Veterinary Services Laboratories (NVSL) confirmed the presence of H6N2 through virus isolation in a pool of five samples of the 11 samples collected from wild green−winged teals in the Rice Lake Conservation Area of Fulton County, IL. Initial screening results announced on September 29 indicated that H5 and N1 subtypes might be present in the collected samples, but further testing was necessary to confirm the H and N subtypes as well as pathogenicity.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/10/0417.xml

[Return to top]

Food Sector

24. *October 18, Food Navigator* — **Cocoa strike disrupts supply.** Cote d'Ivoire cocoa growers have downed tools over pay disagreements, beginning a strike which could dramatically cut supplies to chocolate manufacturers. The strike started this week with farmers in the Anaproci trade union preventing cocoa shipments from reaching exporters warehouses. Disruption in the supply of cocoa is an issue that continues to dog the industry with sales vulnerable to losses caused by civil war, disease and labor concerns. Anaproci represents 80 per cent of the Cote

d'Ivoire's cocoa farmers who produce around 1.3 million tons of the bean annually. The organization called for the strike to demand higher payments and greater financial support for growing co−operatives after low harvest season prices were set. Now farmers have begun burning beans and blocking roads while previously secured shipments are being kept under police guard. The recent unrest follows a warning this week that the swollen shoot virus has been decimating cocoa trees in the region, further lowering supplies.
Source: http://www.foodnavigator.com/news/ng.asp?n=71367−cocoa−strik e−cote−d−ivoire

25. *October 18, Indiana Ag Connection* — **Salad plant to close after spinach scare.** A northern Indiana salad processing plant with about 200 workers is being closed because of what its owner said is a troubled food industry after the nationwide spinach recall stemming from an E. coli outbreak. Ready Pac Produce Inc., which produces fresh−cut salads, fruits and vegetables, plans to stop production next month at its plant in Plymouth about 20 miles south of South Bend, company officials said. The Irwindale, CA−based company had filed on September 6 a layoff warning with the Indiana Department of Workforce Development, saying that 244 jobs could be cut at the plant.
Source: http://www.indianaagconnection.com/story−state.php?Id=693&yr =2006

26. *October 18, Agricultural Research Service* — **Nonthermal food processing.** Technologies such as high−pressure processing, ultraviolet light and irradiation can be faster, cheaper and less disruptive to food quality than traditional thermal processing for killing microbes that can contaminate food products, according to scientists with the Agricultural Research Service (ARS). Under the guidance of research leader Howard Zhang, scientists at ARS' Eastern Regional Research Center (ERRC) in Wyndmoor, PA, have investigated the effectiveness of these and other antimicrobial methods. High−pressure processing (HPP) treatment involves applying 80,000 to 130,000 pounds per square inch of pressure to a sample. The researchers found that applying that extreme pressure for two to five minutes will inactivate the majority of microorganisms on or in a food source. The scientists have also investigated ultraviolet (UV) light and irradiation to protect food. They used UV processing on an apple cider sample that had been inoculated with bacteria. The UV treatment compared favorably to heat pasteurization, reducing the pathogen populations by more than 99 percent without changing the cider's flavor. Irradiation exposes food to a low level of ionizing radiation to inactivate molds, yeasts, parasites, bacteria and other microorganisms that can lead to food spoilage and illness.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

27.

October 18, St. Louis Post Dispatch (MO) — **Air quality test finds rare bacteria.** A routine test of air quality near Busch Stadium in St. Louis, MO, on Monday, October 16, turned up traces of a rare and potentially fatal bacteria that federal officials have warned could be used by terrorists as a biological weapon. However, follow−up tests on Tuesday, October 17, found no evidence of the bacteria, tularemia, which also is called rabbit fever. The bacteria is found naturally in Missouri.
Tularemia information: http://www.bt.cdc.gov/agent/tularemia/index.asp
Source: http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscityco unty/story/BF9047AE28AB59A78625720B0011010C?OpenDocument

28. *October 18, Associated Press* — **Potential pandemic vaccine protects against different H5N1 bird flu strains.** Human trials indicate an H5N1 bird flu vaccine developed using a virus isolated in Vietnam can neutralize antibodies from H5N1 viruses found in other countries, the vaccine's manufacturer said Wednesday, October 18. The preliminary trial results raised hopes that vaccines based on older H5N1 bird flu strains might prove effective against future variants of the virus in the event of a pandemic. In Sanofi Pasteur's trial, 300 volunteers were vaccinated with a strain of the virus isolated in Vietnam in 2004. Antibodies were then examined from their blood, and tests were done using H5N1 viruses from Turkey and Indonesia. The results indicated that the volunteers' antibodies were able to neutralize the other H5N1 viruses, proving that some measure of cross−protection is possible. Klaus Stohr, the World Health Organization's top official on pandemic influenza vaccines, said that while tests in mice and ferrets had suggested that cross−protection might be possible, this is the first evidence available from human trials.
Source: http://www.iht.com/articles/ap/2006/10/18/europe/EU_MED_Pand emic_Vaccine.php

29. *October 17, National Institutes of Health* — **Experimental vaccine protects mice against 1918 flu virus.** Federal scientists have developed a vaccine that protects mice against the killer 1918 influenza virus. They also have created a technique for identifying antibodies that neutralize this virus, a tool that could help contain future pandemic flu strains. These findings are important, the researchers say, to understanding and preventing the recurrence of the H1N1 influenza virus that caused the 1918 pandemic and to protecting against virulent flu strains in the future, including the H5N1 avian flu virus. The 1918−1919 influenza pandemic was the most deadly flu outbreak in modern history, killing 50 million or more people worldwide. Using the genetic sequence information for the 1918 flu virus, scientists created plasmids −− small strands of DNA designed to express specific characteristics −− carrying genes for the virus' hemagglutinin (HA) protein, the surface protein found in all flu viruses that allows the virus to stick to a cell and cause infection. The researchers created two types of plasmids: one to reflect the HA found in the original 1918 flu virus; the other an altered HA protein designed to attenuate (weaken) the virus. Mice were then injected with a DNA vaccine containing both types of plasmids to determine whether they would generate immune responses to the 1918 virus.
Source: http://www.nih.gov/news/pr/oct2006/niaid−17.htm

30. *October 17, Agence France−Presse* — **Mobile phones harnessed in the battle against disease.** Pilot projects are being carried out in Rwanda and Indonesia to develop a mobile phone software that can be used in the fight against HIV/AIDS, avian flu and potential health pandemics. An application is being developed that will allow health workers in the field to use

handheld devices to submit critical health data to authorities in real time. The aim is to allow health workers to use their mobile phones to report disease outbreaks, drug inventory levels, patient treatment status and other important information to a health management information system.
Source: http://news.yahoo.com/s/afp/20061017/hl_afp/singaporetelecomhealth_061017131651;_ylt=AvwVnj33_lkeAhMBs0COokGJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *October 18, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Hawaii Earthquake Update: As of 11:00 p.m. EDT Tuesday, October 17, the Federal Emergency Management Agency (FEMA) Region 9 Regional Response Coordination Center stood down from the Hawaiian Earthquake response operations and returned to normal duties. FEMA 1664−DR−HI operations will be under the direction of the Federal Coordinating Officer Michael L. Karl, in Hawaii. Response and recovery activities continue in the aftermath of the magnitude 6.7 earthquake off Puuanahulu in the County of Hawaii. Over 100 aftershocks have been recorded ranging from 1.7 to 4.4 magnitudes. The majority of damages are in the counties of Hawaii and Maui. Damaged inventory include structures (private and public) and public roads and highways. Power has been restored in Hawaii and Honolulu counties. The state Emergency Operations Center (EOC) and Hawaii County EOC is activated and operating 24 hours/day. Other Earthquake Activity: On Tuesday, October 17, at 3:37 a.m. EDT a magnitude 4.9 earthquake occurred 50 miles north north−west of Chase, AK. There were no reports of damage or injuries. On Tuesday, October 17, at 9:53 a.m. EDT a magnitude 4.9 earthquake occurred 80 miles west of Petrolia, CA. There were no reports of damage or injuries.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat101806.shtm

32. *October 17, Federal Emergency Management Agency* — **President declares major disaster for Hawaii.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency announced that federal disaster aid has been made available for Hawaii to supplement state and local recovery efforts in the area struck by an earthquake that occurred on Sunday, October 15, and related aftershocks.
For more information: http://www.fema.gov/news/event.fema?id=7205
Source: http://www.fema.gov/news/newsrelease.fema?id=30840

33. *October 16, Arlington County* — **Arlington emergency radio station launches.** Arlington, VA, residents can now tune into 1700AM Arlington, a new emergency radio station with the

capability of providing up−to−the−minute information during an incident or emergency. At an official launch event on Monday, October 16, the new station began broadcasting. The Office of Emergency Management has been working on this project for more than two years, securing the necessary Federal Communications Commission licenses, finding a site for the antenna, obtaining the equipment and building the infrastructure. With a single antenna and transmitter, 1700AM Arlington produces a signal capable of being received anywhere in the county. During power outages, 1700AM Arlington runs on a generator. The station equipment is located in two redundant secure locations in county facilities.
Source: http://www.arlingtonva.us/Departments/Communications/6867.as px

[Return to top]

Information Technology and Telecommunications Sector

34. *October 18, WRAL (NC)* — **BellSouth regional outage affects 3.3 million customers.** Some 3.3 million BellSouth high−speed Internet access customers were not able to get online due to a massive outage that lasted more than 12 hours. Digital subscriber line (DSL) subscribers lost their Internet connectivity Monday night, October 16, at 11:30 p.m. EDT, and the outage continued into Tuesday afternoon. The network was restored at around 1 p.m. EDT. The outage did not affect voice call capability. BellSouth attributed the DSL outage to a "network element" but would not define the outage in any further detail. All services, including premium FastAccess DSL Xtreme, were affected across the nine−state BellSouth coverage area.
Source: http://www.wral.com/news/10096538/detail.html

35. *October 18, VNUNet* — **Spoof Microsoft IE7 e−mails install Trojan.** Security experts have detected a malicious Trojan downloader being distributed in spoofed e−mail messages claiming to be from Microsoft. The e−mail appears to come from support@microsoft.com, and offers a link to download Release Candidate 1 of Microsoft Internet Explorer 7 (IE7). Clicking on the link provided in the bogus e−mail launches a maliciously crafted Website that looks very similar to a legitimate Microsoft page. However, security firm SurfControl warned that the Website installs a Trojan via a browser exploit targeted at IE and effectively creates a backdoor on infected systems.
Source: http://www.vnunet.com/vnunet/news/2166697/spoof−microsoft−ie −emails

36. *October 18, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−291A: Oracle updates for multiple vulnerabilities.** Oracle has released patches to address numerous vulnerabilities in different Oracle products. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial−of−service.
Solution: Apply the appropriate patches or upgrade as specified in the Critical Patch Update − October 2006. Note that this Critical Patch Update only lists newly corrected vulnerabilities: http://www.oracle.com/technology/deploy/security/critical−pa tch−updates/cpuoct2006.html
The October 2006 CPU lists 35 vulnerabilities affecting Oracle Application Express. These vulnerabilities are addressed in Oracle Application Express version 2.2.1. Oracle Application Express users are encouraged to upgrade to version 2.2.1 as soon as possible: http://www.oracle.com/technology/products/database/applicati on_express/download.html
Vulnerabilities described in the October 2006 CPU may affect Oracle Database 10g Express

Edition (XE). According to Oracle, Oracle Database XE is based on the Oracle Database 10g Release 2 code.
Patches for some platforms and components were not available when the Critical Patch Update was published on Tuesday, October 17. Please see MetaLink Note 391563.1 (login required) for more information about patch availability:
https://metalink.oracle.com/metalink/plsql/f?p=200:37:826767
3867231248703:::p_database_id,p_id:NOT,391563.1
Known issues with Oracle patches are documented in the pre−installation notes and patch readme files. Please consult these documents and test before making changes to production systems.
Source: http://www.uscert.gov/cas/techalerts/TA06−291A.html

37. *October 17, CNET News* — **FBI director wants ISPs to track users.** FBI Director Robert Mueller on Tuesday, October 17, called on Internet service providers (ISPs) to record their customers' online activities, a move that anticipates a fierce debate over privacy and law enforcement in Washington next year. "Terrorists coordinate their plans cloaked in the anonymity of the Internet, as do violent sexual predators prowling chat rooms," Mueller said in a speech at the International Association of Chiefs of Police conference in Boston. Law enforcement groups claim that by the time they contact ISPs, customers' records may have been deleted in the routine course of business. Industry representatives, however, say that if police respond to tips promptly instead of dawdling, it would be difficult to imagine any investigation that would be imperiled. It's not clear exactly what a data retention law would require. One proposal would go beyond Internet providers and require registrars, the companies that sell domain names, to maintain records too.
Source: http://news.com.com/FBI+director+wants+ISPs+to+track+users/2
100−7348_3−6126877.html?tag=nefd.top

38. *October 17, Reuters* — **Study: Workers often jot down passwords.** One in three people write down computer passwords, undermining their security, and companies should look to more advanced methods, including biometrics, to ensure their systems are safe, a new study shows. A study released on Tuesday, October 17, by global research firms Nucleus Research and KnowledgeStorm found companies' attempts to tighten IT security by regularly changing passwords and making them more complex by adding numbers as well as letters had no impact on security. Staff still had a tendency to jot down passwords either on a piece of paper or in a text file on a PC or mobile device. The study, which surveyed 325 U.S. employees, found that a single sign−on system is just as effective as more complex schemes and that user education on the importance of proper password protection did not deter employees from their lax habits.
Study: http://www.nucleusresearch.com/research/g68.pdf
Source: http://news.com.com/Study+Workers+often+jot+down+passwords/2
100−1029_3−6126924.html?tag=nefd.top

39. *October 17, IDG News Service* — **Hackers' project disguises security−busting code.** Hackers are developing new software that will help hide browser attack code from some types of security software. The software, called eVade o' Matic Module (VoMM), uses a variety of techniques to mix up known exploit code so as to make it unrecognizable to some types of antivirus software. The software uses server−side scripting technology to create new versions of the exploit code, which then get delivered to browser users when they visit the attacker's

Website. By making a number of cosmetic changes to the code that do not affect its functionality, VoMM creates a new version of the malicious software that cannot be detected by "signature−based" techniques. Signature−based antivirus products analyze known malware and then create a digital fingerprint that allows the antivirus software to identify malicious code. By adding extra components that are not included in known signatures, VOMM creates software that can evade detection.
Source: http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9004218

40. *October 17, CNET News* — **Windows virus affects some Apple iPods.** Apple Computer warned on Tuesday, October 17, that some of its latest iPods have shipped with a Windows virus. The company said that a small number of video iPods made after September 12 included the RavMonE virus. It said it has seen fewer than 25 reports of the problem, which it said does not affect other models of the media player, nor does it affect Macs.
Source: http://news.com.com/Windows+virus+worms+onto+some+Apple+iPods/2100−7349_3−6126804.html?tag=nefd.top

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	32947 (−−−), 1026 (win−rpc), 6881 (bittorrent), 4662 (eDonkey2000), 2234 (directplay), 113 (auth), 139 (netbios−ssn), 445 (microsoft−ds), 1111 (lmsocialserver), 50001 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

41. *October 17, New York Times* — **Wal−Mart acquiring chain in China.** Wal−Mart Stores, the largest retailer in the United States, is laying the groundwork to become the biggest foreign chain in China with the $1 billion purchase of a major retailer in Shanghai. The move represents a large step for Wal−Mart's strategy in China, allowing the American retailer to more than double its presence in a country that, despite its size and growing middle class, remains largely untapped by foreign retailers. Though the size of the acquisition −− of a Taiwanese−owned supermarket chain called Trust−Mart −− may be modest for Wal−Mart, it is a critical one because the Chinese market is becoming much more pivotal in the retailer's overall international strategy. For Wal−Mart, China represents an opportunity to tap a vast and fast−growing market abroad at a time when the company's sales are lagging elsewhere and it has run into obstacles to expansion at home. Wal−Mart expects to close the deal for Trust−Mart by the end of the year, but it still needs approval by Chinese authorities.
Source: http://www.nytimes.com/2006/10/17/business/worldbusiness/17w

almart.html?hp&ex=1161144000&en=c8573d137721ed20&ei=5094&par tner=homepage

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer